BUSINESS KNOWLEDGE KEY TO ENSURING PDPA COMPLIANCE, SAY DPOS

Data Protection Officers take on the tall order of marrying business knowledge with an understanding of the PDPA to ensure compliance for their organisations.

Under the PDPA, organisations are required to designate at least one individual, the Data Protection Officer (DPO), to oversee the organisation's data protection responsibilities and ensure compliance with the PDPA.

At Emergenetics International – Asia Pacific (EGI-A), an organisational development consultancy, Deputy Chief Executive Officer, Mr Colin Yeow, takes on this role. Explaining how this came about, he said: "We decided early on that the DPO had to be a member of the management team. This is to reflect the importance we place on data protection, and also allow changes to policies and processes to be effected."

While Mr Yeow is the designated DPO, the company also agreed that the changes required for PDPA compliance cannot be pushed through by one individual as the policies and practices will affect different processes and departments throughout the organisation.

A DPO Management Team was thus created. The company's Chief Operating Officer takes care of establishing policies and processes; the Chief Executive Officer takes care of key stakeholder communications; the Creative Director handles database management and IT security; and Mr Yeow himself is in charge of partner communications.

At Protiviti, a consulting firm which focuses on Internal Audit, IT Consulting, Risk & Compliance and Financial Services, ensuring PDPA compliance is also a team effort. Its Human Resources Manager, Ms Dorothy Yeo, is the DPO tasked with ensuring that data protection policies and practices within the company are in compliance with the PDPA. She works with a task force comprising herself, a practice director, and leads from the finance and IT departments.

"The immediate responsibility of the team was to put in place a formal process for the collection, usage and storage of all personal data in the company. That also included establishing a formal procedure to handle request for access to personal data."

- Ms Dorothy Yeo,
Human Resources Manager

KNOW THE BUSINESS

The fact that the composition of both DPO teams mirrors their organisations' business structure is no coincidence. Having insights into the nature of the business, knowing what the different departments do and understanding their processes are "fundamental" to the DPO role, said Ms Yeo.

A background in compliance and governance is also useful, said Mr John Ho Chi, Partner of Advisory Services at professional services firm EY. To get DPOs up to speed in this respect, courses such as the "Introduction to the Fundamentals of the Personal Data Protection Act (PDPA) for Non-Legal Personnel" have been developed under the Business Management Workforce Skills Qualifications (BM WSQ) framework to help DPOs to deepen their understanding of PDPA.

MAPPING OUT THE PERSONAL DATA INVENTORY

As organisations embark on their compliance journey, one of the things that the DPOs need to do is to map out their personal data inventory. This should include personal data in both electronic and non-electronic forms.

DPOs should also review their organisation's data management framework and processes to align them with the PDPA. This includes determining how, when and where the organisation collects personal data, the purposes for the data collection, and ensuring that consent has been obtained for the collection, use and disclosure of the data.

The setting up of a Protiviti DPO task force was one of the first things that was looked into. "The immediate responsibility of the team was to put in place a formal process for the collection, usage and storage of all personal data in the company. That also included establishing a formal procedure to handle request for access to personal data," said Ms Yeo.

ASSESSING RISK

The personal data inventory is also the starting point for developing an appropriate and consistent risk management framework for the handling of personal data, said Mr Ho of EY.

DPOs are encouraged to conduct a risk assessment exercise to flag out any potential data protection risks, and put in place data protection policies to mitigate those risks.

For example, the organisation may wish to consider carrying out regular internal audits to ensure that its processes adhere to the PDPA and if there is a breach, there should be processes and measures in place to respond to such situations.

DEVELOPING POLICIES

The next important area that the DPO has to look into is the development of policies and practices to handle personal data.

As global companies, both EGI-A and Protiviti are able to leverage policy guidelines issued by their corporate headquarters, albeit with some fine-tuning to address the local requirements of the PDPA.

An example was the use of employees' photographs and names on the company's marketing and social media channels such as the Protiviti Facebook page. "We have to be more specific in telling the staff how we are going to use the data and they have to sign a form to acknowledge this," said Ms Yeo.

To make these changes, members of Protiviti's data protection team set aside time from their primary job scope to work on the personal data protection compliance exercise. "I would say when we first started, it took us about three months to complete the initial compliance framework," said Ms Yeo.

For EGI-A, the corporate policy guidelines that were already in force also meant that the company was in compliance with most of the requirements of the PDPA. However, some processes had to be tweaked because as a global company, EGI-A also collected information from an online source based in the United States (US). "Thankfully, none of the changes we made were complex ones as our US office is also very strict about their privacy policy and confidentiality," said Mr Yeow.

"What EGI-A focused on was to ensure that its policy manual for Singapore partners and customers was re-written to reflect the PDPA and to send out a communication piece highlighting this policy change. These efforts didn't involve any cost on our end, and perhaps just a short meeting among our management team to ensure that the policy amendments were clear and accurate," said Mr Yeow.

COMMUNICATING WITH STAKEHOLDERS

After its initial audit of existing processes and the decision to tighten some of its data-handling procedures, EGI-A had to make sure that the comprehensive plans and adjustments were communicated to its stakeholders simply. "To do this, we had to understand how our different stakeholders would perceive the message and pre-empt some of the questions that might arrive," said Mr Yeow.

Emphasising the importance of communications skills, Mr Yeow said it allows the DPO team to gain buy-in from colleagues who may be on the front line collecting personal information. "We need to know what they are doing and how they are doing their work, and also be able to provide feedback, advice and ask the right questions for them to think about data protection as they work."